Cyber Security Resources

A CIRMA Risk Management Best Practices Guide

CIRMA

Cyber Security Resources - A CIRMA Risk Management Best Practices Guide

1st edition

This publication is intended for general purposes only and is not intended to provide legal advice. If you have questions about particular legal issues or about the application of the law to specific factual situations, CIRMA strongly recommends that you consult your attorney.

Cyber Security Resources

A Risk Management Best Practices Guide

Table of Contents

Introduction

In March 2013, the nation's top intelligence officials cautioned that cyber-attacks and digital spying would be principal threats to national security.

Cyber security is important because government and educational entities collect, process, and store enormous amounts of data on computers and other devices. A significant portion of that data is classified as sensitive personal identifiable information (PII), like social security numbers, bank account information, credit card information, and student information protected by the Family Educational Rights and Privacy Act (FERPA), all of which unauthorized access or exposure could have negative consequences.

Because Municipalities and School Districts transmit sensitive data across networks and to other devices in the course of doing business, there is a significant need for robust cyber security protocols. As cyberattack volume and sophistication increase, members need to act to protect their sensitive data.

I. Cyber Security Facts and Trends

The Important Cyber Facts of 2020[1]

- In 2020, 80% of businesses have seen an increase in cyber attacks
- A cyber-attack is attempted every 39 seconds
- 700 million people in 21 countries have experienced some form of cybercrime
- The damage related to cybercrime is projected to hit $6 trillion annually by the end of 2021
- Ransomware attacks rose 148% in March 2020
- Cloud-based attacks rose 630% between January and April 2020
- More than 80% of reported cyber-attacks are phishing
- Phishing attempts have increased by more than 660% since March 1, 2020
- A cyber-attack is rarely a single, isolated event but a recurring and chronic issue. From 2018 to 2019, known attacks on local governments rose 58.5%[2]

8 Most Common Causes of Data Breach[3]

- Weak and stolen credentials, a.k.a. passwords
- Back doors, application vulnerabilities
- Malware
- Social engineering
- Too many permissions
- Insider threats
- Improper configuration and user error

2021 Cybersecurity Trends to Watch For[4]

The year 2020 brought with it both trials and triumphs. COVID-19 has forced companies to create and maintain remote workforces and operate off of cloud-based platforms. The rollout of 5G has made connected devices more connected than ever. All this to say, the cybersecurity industry has never been more critical. These recent events and the below cybersecurity statistics and figures considered, here are some industry trends and predictions to watch for in 2021 and beyond.

- Remote workers will continue to be a target for cybercriminals
- As a side effect of remote workforces, cloud breaches will increase
- The cybersecurity skills gap will remain an issue
- As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber-attacks
- Remote devices reentering municipal and school district networks

Cyber Security Defined

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be called ‘information technology security.[5]

[1] https://www.idagent.com/10-essential-facts-about-cybercrime-in-2020

[2] https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf

[3] https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/

[4] https://www.varonis.com/blog/cybersecurity-statistics/

[5] Merriam-Webster Dictionary - https://www.merriam-webster.com/dictionary/cybersecurity

II. Background

The Verizon Data-Breach report investigated 32,002 cyber-security incidents resulting in 3,950 confirmed breaches. It was determined that 70% of these confirmed breaches were caused by outsiders. While data espionage may receive extensive media coverage, the reality is that 86% of all ransomware attacks are financially motivated.[6]

Cyber-attacks involving large corporations like Facebook and Marriott continued to make headlines. But cyberattacks are not limited to the private sector. One of the biggest cybersecurity stories to make the news involved the city of Atlanta, which sustained the largest cyberattack against a major U.S. city.[7]

In March of 2018, Atlanta was the victim of a remote ransomware attack in which anonymous hackers disabled online access, encrypted files, and demanded a $51,000 ransom, payable in Bitcoin, in exchange for the decryption key to regain access to system files. City officials refused to pay the ransom and, recovery from the attack cost the City of Atlanta millions of dollars. The attack took many of the city's services offline for nearly a week and disrupted services and critical functions. The fallout from the attack included loss of a years' worth of bodycam and police dashcam recordings, the municipal court system was unable to access electronic records, WiFi at Atlanta's Hartsfield-Jackson International Airport was shut down, the city's online bill payment system was disabled, and several departments, including the police, were forced to file reports on paper instead of electronically.

Cyberattacks against municipalities are increasingly common and becoming more sophisticated and severe. The need for cybersecurity becomes more urgent as more local governments adopt new technologies and offer services that are integrated with online networks. Cities and towns across the country are being targeted by cybercriminals, nation-states, and hacktivists who seek the path of least resistance by exploiting vulnerabilities in municipal computer networks.[7]

Taking a strategic, holistic approach to cyber security will reduce the potential of an attacker being successful. The Risk Management Framework provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.

Because local governments store and maintain an extraordinary amount of personal, confidential, and sensitive information, they are a prime target for cybercriminals to launch malware or data-retrieval attacks. As a result, government agencies have lost millions of citizen records since 2009. Although the responsibility for cyber security may seem overwhelming and sometimes bewildering, as with any exposure, it can be managed through appropriate risk management techniques and specialized insurance programs.

Risk Identification

Risk identification is the process of identifying and assessing threats to municipalities and school districts, also encompassing their operations and workforce. This can include assessing IT security threats such as malware and ransomware, end-user exposures, unintentional data loss, accidents, natural disasters, and other potentially harmful events that could disrupt a municipality's or school district's ability to provide services to its communities and residents.

[6] Verizon Data-Breach Report - https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

[7] https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities#:~:text=A%20good%20starting%20point%20in%20preventing%20cyberattacks%20and,problem%20that%20can%20be%20solved%20by%20technology%20alone.

III. Challenges of Cyber Security[8]

In order to implement an effective cyber security program, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber security encompass all of the following components:

- **Network security:** The process of protecting a network from unwanted users, attacks, and intrusions.
- **Application security:** Apps require constant updates and testing to ensure these programs are secure from attacks.
- **Endpoint security:** Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company's network.
- **Data security:** Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.
- **Identity management:** Essentially, this is a process of understanding every individual's access in the organization.
- **Database and infrastructure security:** Everything in a network involve databases and physical equipment. Protecting these devices is equally important.
- **Cloud security:** Many files are in digital environments or "the cloud." Protecting data in a 100% online environment presents a large number of challenges.
- **Mobile security:** Cell phones and tablets involve virtually every type of security challenge in and of themselves.
- **Disaster recovery/business continuity planning:** In the event of a breach, natural disaster or other event, data must be protected and business must go on. For this, you'll need a plan.
- **End-User:** An end-user is an individual who uses hardware or software programmed or designed by another person who does not support that product. Most computer users are considered end-users in one capacity or another.[9]
  - **End-user education:** Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes, 2-factor authentication, etc.) is an important part of cybersecurity.

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known threats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations were created to promote more proactive, uniform, and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security instead of the traditional perimeter-based model.

Some security researchers label end-users as the biggest threat to cyber-security. Unlike applications that can be patched or systems that can be hardened, end-users continue to expose IT systems and frameworks to serious security threats. "Security is fundamentally a human issue," says Scott Crawford, an analyst at Enterprise Management Associates in Boulder, Colo. "Human nature can be totally unpredictable, so when it comes to IT, the risk posture changes every day." (DeCarlo, 2007)

[8] Digital Guardian - https://digitalguardian.com/blog/what-cyber-security

[9] www.computerhope.com/jargon/e/enduser.htm#:~:text=An%20end%20user%20is%20an%20individual%20who%20uses,unless%20you%20designed%20the%20hardware%20or%20software%20yourself.

Questions to Consider

As you proceed through the risk management process, there will be many issues that should be considered and questions to be answered; for example:

- What are the rules that will govern the use of Town or School owned devices and resources? (i.e., computers, smartphones, tablets, etc.)
- What training should be available to staff, and how will it be delivered?
- If there is a cyber event (malware, spyware), who should be contacted in the organization?
- What is the policy on bringing personal devices into the workplace?
- What devices are allowed to connect to the organization's systems, and could the device infect or weaken the system security?

Examine the Risk

This establishes the probability that an event may occur and the potential outcome of each event. Applying data from resources such as the Verizon data breach reports, the Connecticut Intelligence Center, and other trusted resources allow municipalities to understand the risks and examine each potential of each risk.

- Another term commonly used is "Risk Mapping." The purpose is to map out where your vulnerabilities exist in your municipalities and schools and to gain some idea of how often they arise and to what extent the impact of the risks will have in the future. Risk Mapping involves a detailed examination of the identified risks and exposures. Several questions are considered when ranking the impact of the event; they include:
  - **The likelihood of occurrence:** Will the municipality be targeted by cybercriminals?
  - **The scope of impact:** If we are attacked with ransomware, what systems could be affected?
  - **The frequency of occurrence:** How often can this occur?
  - **The potential size of the affected area:** How many servers are interconnected?
  - **Population impact:** What business-critical functions could be affected, and additionally, impact our most vulnerable systems? How will this impact our residents?

A valuable part of this process is the hypothetical consideration of "worst-case scenarios" by imagining what would happen if the worst possible catastrophe involving one or more events were to occur). A cyber-attack may result in:

- Unauthorized access to servers and computers
- Unauthorized access to software, hardware, and networks
- Loss of data/deletion or modification of data
- Unsecured portable devices and computers

The Risk of Human Error

After risks to the computers and network systems from outside threats, one of the most common and costly cyber risks to most municipal and school operations comes from unsafe cyber practices by their own employees and vendors. Even the sophisticated security systems can be compromised by an employee who unintentionally clicks on a link in a phishing email that accidentally installs malicious pieces of software, such as ransomware, that can take over a network, computer, or communication system.

- It is estimated that **one in five employees** will inadvertently click on a "bad" link.

Human error remains a significant point of vulnerability and one that municipali¬ties and schools should address early on. Below are some simple best practices to implement which may reduce this risk:

End-User Training

A member's cyber security is only as strong as the weakest link. While it is possible to make significant investments in software, hardware, and services to help prevent cyber-attacks, the most important preventative measure is end-user training. As attackers are always searching for new ways to get around safeguards, they find that engaging the end-user is easier than trying to find holes in the technology. It is important that members take proactive measures to ensure all staff members are up to speed on the basics of cybersecurity.

The end-user is usually the weakest link when it comes to cybersecurity and that is what attackers are counting on. This is particularly why phishing is such a popular technique for spreading ransomware. The attackers may be unable to get past the hardware, software, and trained technical staff, but can easily access your untrained non-technical staff in the hopes they will be gullible enough to take the bait. If your staff is not properly trained to recognize the risks your data may be in jeopardy.

A good end-user security training program is an inexpensive way to enhance security in your municipality or school district. Below are some tips for a successful end-user training program:[10]

- The information contained in the content of the training must be delivered in a "language" that a non-technical person would understand.
- The training topics should give the information to the end-users at a pace and in a time frame that where they can be focused on the material.
- Trainings should not be too long. Training that "drags" on will discourage staff from taking the course and limit the amount of information retained.
- Try to make the trainings interactive and engaging.
- Training should include what to do if an end-user suspects that their device has been compromised or believe that there is suspicious activity occurring on their devices.

Your Computer System

Outdated

Obsolescence is a serious risk. Aging hardware and software not only can put a single system at risk but could put everyone else on your network at risk. Outdated hardware and software can create vulnerabilities that criminals can take advantage of to breach systems. Not only do you have to worry about individuals creating windows of opportunity, but now there's the chance that simply using your software or equipment—because it's outdated—could create weak spots for hackers to exploit your network security.

Most major software vendors publish their support life cycle and end-of-life policies, so customers are aware of the date at which the product will cease to receive periodic updates such as security patches or when technical support is gradually phased out and no longer available. This makes it easier to plan and manage a technology refresh well in advance.[11]

Software Patching

Software updates are important to your digital safety and cyber security. The sooner you update, the sooner you'll feel confident your device is more secure — until the next update reminder.[12]

Why are software updates so important? There are a lot of reasons. According to Norton.com, here are five reasons why it's important to update software regularly;

1. **Software updates do a lot of things**
    a. Software updates offer plenty of benefits. It's all about revisions. These might include

[10] Lawrence King, Application Analyst, Northwestern Medical Center - https://www.cyberdefensemagazine.com/end-user-security-education/

[11] https://sites.northwestern.edu/thesafe/2018/07/24/your-old-computer-is-a-security-risk/

[12] https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html

   repairing security holes that have been discovered and fixing or removing computer bugs. In addition, updates can add new features to your devices and remove outdated ones.

   b. It's also a good idea to make sure your operating system is running the latest version.

2. **Patches help reduce/eliminate security flaws**
   a. Hackers love security flaws, also known as software vulnerabilities. A software vulnerability is a security hole or weakness found in a software program or operating system. Hackers can take advantage of the weakness by writing code to target the vulnerability. The code is packaged into malware — short for malicious software.

   b. Software updates often include software patches. They cover the security holes to keep hackers out.

3. **Software updates help protect your data**
   a. Personally identifiable information (PII)— from emails to bank account information — is valuable to cybercriminals. They can use it to commit crimes in your name or sell it on the dark web to enable others to commit crimes. If it's a ransomware attack, they might encrypt your data. You might have to pay a ransom for an encryption key to get it back. Or, worse, you might pay a ransom and not get it back.

4. **It's not all about you**
   a. If your device gets a virus, it could pass it on to anyone that is connected to the same network, including through your home network. A trusted security program can help keep your devices secure. And that can potentially help all those people you interact with online. But it's also important to know antivirus protection isn't enough to protect your devices against all cyberthreats.

5. **You deserve the latest and greatest**
   a. Updates not only patch security holes they can also add new features and improve existing ones. In that way, software updates are all about protecting your network. Software programs may get a new shot of stability — no more crashing. Or an update might boost program performance — more speed.

   b. To reduce the reliance on the end-user "clicking ok" when prompted to update the software, it is recommended that municipal and school district devices be configured to update automatically.

Forward/Public-facing Applications and Servers

This term refers to any free or paid application or system that the public can access. Also called "customer-facing," information systems often comprise a public-facing component as well as a private side that is available only to the internal staff, such as "Remote Desktop Protocols (RDP)."

However, there is a vulnerability in the method used to encrypt sessions in earlier versions of RDP. This vulnerability can allow unauthorized access to your session using a man-in-the-middle attack. While Remote Desktop is more secure than remote administration tools such as VNC that do not encrypt the entire session, any time Administrator access to a system is granted remotely there are risks. The following tips will help to secure Remote Desktop access to both desktops and servers that you support;[13]

1. Use Strong Passwords
2. Use Multifactor Authentication (MFA)
3. Update software
4. Restrict Access using firewalls

[13] https://security.berkeley.edu/education-awareness/securing-remote-desktop-rdp-system-administrators

5. Enable Network Level Authentication
6. Limit users who can log in using RDP
7. Set an account lockout policy

Third-Party Vendor Agreements[14]

Many municipalities and school districts rely on third party IT professionals to assist with network management, desktop support, and data storage. Since these third-parties are not employees of a CIRMA member, the relationship then becomes based on the executed contractual agreement.

A contract is an agreement with specific terms between two or more persons or entities in which there is a promise to do something for consideration (usually money). Many municipalities that do not wish to assume the risk of an activity or be held primarily responsible (and liable) for any losses caused by that activity may decide to contract out the service. Contracting for services, also known as subcontracting, is a common non-insurance risk transfer method recommended by CIRMA. By contracting for service, a municipality transfers the liability loss exposure to third parties that are better able to control losses generated by a particular activity.

Contracting, in general, is one of the most significant areas of legal concern and can involve variations on circumstances and contain many complexities. Although many “standard” agreements and contracts are available for use, no single contract or agreement should ever be considered “standard.” There are always opportunities to identify potentially unfavorable terms and negotiate changes and modify the terms and conditions of these documents before signing them, even if a third party implies otherwise. An essential part of contracting with a third party is knowing and identifying ahead of time what requirements or changes need to be made in a contract or agreement to protect the interests of the municipality adequately. It is recommended that language be contained within each agreement that clearly identifies the third parties’ responsibilities as a result of a cyber incident, to include requirements outlined in Conn. General Statutes. Additional language should be included that provides indemnification and hold harmless language that benefits the municipality or school district in the event of a cyber incident.

As a best practice, entities should have policies and procedures for the review and authorization of contracts and agreements entered into on the municipality’s behalf. Third-party vendor agreements and contracts should be reviewed prior to signing in order to ensure a municipality’s interests are adequately protected, or, in the event no changes can be made, be aware of potential risks that may be involved. This process should empower municipal employees, including those with contracting authority, to make decisions with which they may not be comfortable or knowledgeable enough to make alone.

- **Members should consider utilizing CIRMA’s Contract Review service prior to executing any third-party cyber / IT contracts.**

Access Privileges

Privilege misuse is a top cybersecurity threat today that often results in expensive losses and can even cripple businesses. It's also one of the most popular attack vectors among hackers because when successfully carried out, it provides free access to an enterprise's underbelly, often without raising any alarms until the damage is done.[15] Permissions enable you to fine-tune your network security by controlling access to specific network resources, such as files or printers, and with respect to individual users or groups, permissions can also enable some users to read certain files but not modify or delete them.

- It is a recommended practice to identify what access each network user should have. This can reduce the likelihood of a virus, malware, etc., from gaining complete access to business-critical applications and servers.

[14] CIRMA Risk Management Risk Transfer Best Practices Guide.

[15] https://www.manageengine.com/privileged-access-management

Working Remotely

Amidst these uncertain times, more people have been working remotely than ever before. These unprecedented circumstances require your Information Technology (IT) Departments to work diligently to ensure that your employees can be productive and continue to deliver critical community services while working from home.

One particular area of focus must be on your network's cyber security. Regrettably, the Coronavirus pandemic is an unfortunate event specifically targeted by criminals preying on and exploiting people's fears to increase their chances of phishing, ransomware attacks, and other methods of stealing personally identifiable information (PII) and exfiltrating data from their networks.

CIRMA has recently shared alerts on specific, criminal, and foreign, state-driven activities to carry out nefarious acts against your networks. In order to continue to assist you in defending your networks during this intense time, below are best practices pertaining to specific topics that can help keep your networks secure while your employees work from home. These and other best practices can also be found on the CIRMA Cyber Resource webpage.

Business Email Compromise (BEC) attacks continue to be the most heavily utilized cybercriminal attack vector. BEC attacks are a form of cybercrime that uses email fraud to attack commercial, government, and non-profit organizations to achieve a specific outcome that negatively impacts the target organization. Examples of common BEC attacks include invoice scams and spear phishing spoof attacks which are designed to gather data for other criminal activities. Often, consumer privacy breaches occur as a result of a BEC attack. Communications to employees should stress that although they are working remotely, any suspicious requests should be verified directly with the requestor directly prior to the release of PII or other sensitive data.

An example of a Business Email Compromise (BEC) would be an email sent to a specific employee within an organization via a spoof email (or series of spoof emails) that fraudulently represents a senior colleague (CEO or similar) or a trusted customer. The email outlines instructions to approve payments or release some type of data. The emails often use social engineering to trick the victim into making money transfers to bank accounts, changing direct deposits, releasing W2s or clicking on links which allow malicious software, known as malware, to be introduced into the town's network.

Wireless Networks (WiFi) (employee's home): Require your employees to regularly change their default password on their wireless network.

WiFi (public): Minimize the use of public WiFi for any of your town or school district-owned member equipment. Advise employees to lock their devices when they step away from their workstations.

Municipal and School District Devices: There may be a need for members to provide devices to employees or students who will be working remotely. A proper inventory of those devices should be kept and monitored on a regular basis. Member IT teams should establish a process to keep software applications on these devices up-to-date which can help detect unauthorized software application installation or use. Policies and protocols should be established to limit or restrict the use of any non-approved software programs.

Personal Devices: Although this may not be the best practice, CIRMA Risk Management offers a comprehensive white paper that outlines best practices for allowing personal devices to be connected to your network.

Employees should practice effective security hygiene at home by keeping their operating systems and software fully up-to-date. Employees should utilize effective anti-virus software, and effective password maintenance for their device(s). In addition, employees should also be advised to take extra precautions and avoid downloading unknown software/applications onto their device(s).

Returning to the Office[16]

The COVID-19 pandemic has created a laundry list of challenges for municipalities and school districts. One that is potentially unnoticed or under-reported is cybersecurity. As individuals return to their office workplaces, it's possible that something malicious is already waiting for them on their devices.

A significant number of employees have been working from home due to government restrictions and recommendations regarding social distancing. However, as restrictions are gradually lifted, employees are slowly returning to the office. And whilst this might be seen as positive, it could be a problem, too. Because we know that home networks are not as secure as commercial networks, it is important to understand that employees may have acquired certain types of malware that have not been "executed" as of yet, simply, it is waiting to be connected to a larger network.

Employees returning to their office will begin to connect their devices to the municipal or school district networks. If cybercriminals have been lying dormant on the devices, this connection will then provide an opportunity to move through these networks, which will potentially lead to data encryption, reputational and regulatory issues.

- While working remotely is not necessarily a new phenomenon, the associated increase has been significant as a result of the COVID-19 pandemic. During this time there has been a substantial rise in mal-spam campaigns distributing malware such as Emotet and Trickbot, among others. These threats can be extremely difficult to detect without strong endpoint visibility and virus protections across employee devices. These capabilities are simply something that many municipalities and school districts may not have. This coupled with the end-users residential wi-fi network and basic protections, make it easy for the cybercriminal to access the devices.

In order to deal with these sorts of threats, municipalities and school districts should look to identify and respond to them by considering to use the latest in next-generation solutions, such as Endpoint Detection and Response tools. These tools utilize behavioral-based approaches to detection. This is a proactive form of cybersecurity. By monitoring activity in the system, the cybersecurity solution can determine normal behavior and recognize dangers from unusual activity

If Endpoint Detection and Response software are not feasible, municipalities and school districts should consider:

- Regularly updating antivirus definitions
- Conduct regular device virus scans
- Conduct regular review of device logs and activity upon re-entering the municipal or school district networks
- Review and update firewall rules, including those that may have been relaxed during a lockdown
- Determine if security patches are completed on a regular basis
- Conduct regular vulnerability assessments; this practice can identify vulnerabilities like unpatched software and the use of weak credentials, that may not have been identified during the lockdown

[16] The Cyber Risk of Remote Working - https://www.tripwire.com/state-of-security/featured/cyber-risks-remote-workers-returning-office/

IV. Managing Cyber Security[17]

While The National Cyber Security Alliance (NCSA), through SafeOnline.org, recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security management across all business practices. NCSA advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected." NCSA's guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization's "crown jewels," or your most valuable information requiring protection; identifying the threats and risks facing that information, and outlining the damage your organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way municipalities collects, store, and secures data. Following a cyber risk assessment, develop and implement a plan to mitigate cyber risk, protect the "crown jewels" outlined in your assessment, and effectively detect and respond to security incidents.

This plan should encompass both the processes and technologies required to build a mature cyber security program. Cyber security best practices must evolve to accommodate the increasingly sophisticated attacks carried out by hackers. Combining sound cyber security measures with an educated and security-minded employee base provides the best defense against cybercriminals attempting to access to your entity's sensitive data. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures.

State and local government is constantly combating the challenge of financial allocation. Long-term damages can exceed tens of thousands of dollars. Less than half of department managers are "moderately/exceptionally aware" of the need for cybersecurity. This lack of knowledge and awareness by governing officials remains a substantial barrier to achieving an adequately protected community. According to a study conducted by the National Association of State Information Officers (NASCIO), about 50% of states do not have a committed cybersecurity line-item budget. Even more concerning is that 37% of states have seen a reduction in funding or no change at all. The lack of reoccurring funding translates to municipal networks and computers being put at risk of increasing cyber threats.[18]

Recommended Best Practices

- Implement a password policy; this is one of the most important best practices
- Train and test staff regularly and repeatedly so that they understand and fully appreciate their role in maintaining a cyber-safe work environment
- Institute strong security rules for vendor access to systems, facilities, and equipment
- Develop strong policies concerning employee access to sensitive information, especially at the separation of employment
- Train employees not to use "plug-in" devices, such as thumb drives, from unfamiliar sources
- Train employees to "lock" their computers when not at their desks
- Institute a strong acceptable-use policy for electronic communication devices equipment
- Implement
- Restrict employee access based on their job descriptions and responsibilities
- Implement a strong Bring-Your-Own-Device policy
- Implement a strong incident reporting protocol for all employees
    - The best way to support your municipal or school cyber security defenses is to ensure that your organization reports incidents through the appropriate channels as soon as they are discovered.

[17] Digital Guardian - https://digitalguardian.com/blog/what-cyber-security

[18] https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf

- Monitor employee behavior to ensure compliance
- Implement Software Patching protocols to identify and secure vulnerable systems
- **Multi-Factor Authentication (MFA):**
    - Multi-factor authentication is an important tool for keeping yourself cyber secure online. These three examples can help you to get started in using multi-factor authentication to protect yourself. https://www.getcybersafe.gc.ca/en/blogs/examples-multi-factor-authentication-action
    - Multi-factor authentication (MFA; encompassing Two-factor authentication or 2FA, along with similar terms) is an electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects the user from an unknown person trying to access their data, such as personal ID details or financial assets. https://en.wikipedia.org/wiki/Multi-factor_authentication

Implementing a Strong Password Policy

Why do strong, unique passwords matter? Because stolen, weak, or default passwords are involved in about 63% of confirmed data breaches according to the Verizon Data Breach Report. Although cyber security experts recommend the use of strong, unique passwords as a top priority, unfortunately this remains one of the least followed recommendations There are several reasons strong passwords are critical to cyber safety.

First, cyber attackers compromise websites and online accounts every day, and post lists of usernames, email addresses, and passwords online. This not only exposes people's passwords, it exposes them with information that uniquely identifies the user, such as an email address. That means that a malicious actor can look for other accounts associated with that same person, such as work, personal social media, or banking accounts. Then they can try with the exposed password, and if the password has been reused, they can gain access.

Secondly, when malicious cyber threat actors can't easily find or guess a password, they may use a technique called brute-forcing, which is a technique where every possible password is attempted until the correct password is identified.

Computers can try thousands of passwords per second, but for this technique to be worthwhile, the malicious cyber threat actor needs an easily identifiable password. The stronger the password, the less likely brute forcing will be successful.

- **Example** - when faced with choosing a password that fits these requirements, most users will pick a word, put the uppercase letter first, and end the password with the number and symbol. Alternatively, many people will replace common letters with a number or symbol that represents that letter. This changes a common password, such as "password," into the only slightly more complex password of "p@ssw0rd," which is still an easy-to-guess pattern.

Recommendations for Creating Strong, Unique Passwords

You may consider using a password manager, an application that can run on a computer, smartphone, or in the cloud that securely tracks and stores passwords. Most password managers can also generate strong, random passwords for each account. As long as the password to access the password manager is strong and unique and utilizes two-factor authentication, this technique can be affective.

If your municipality's cloud-based password manager is compromised, or a vulnerability in their software is discovered and leveraged by an attacker, it is possible that all of the passwords could be compromised. If you choose a password manager that is local to your computer or smartphone, your passwords may be compromised if malware gets on your computer or you lose your smartphone. When choosing a password manager, ensure it is from a known, trustworthy company with a good reputation.

Another technique to assist in building strong, unique passwords is to choose a repeatable pattern for your password, such as choosing a sentence that incorporates something unique about the website or account and then using the first letter of each word as your password. For example:

- "This is my January password for the Center for Internet Security website" would become "TimJp4tCfISw."

This password capitalizes five letters within the sentence, swaps the word "for" to the number "4," and adds the period to include a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern. Variations on this technique include:

- Using the first letters from a line in a favorite song or a poem
- Using just the sentence itself
- Using symbols to replicate numbers and letters

Employees should be reminded that Post-It notes, index cards, etc. aren't secure from attackers even if they might be out of sight under the keyboard.

Report Cyber Incidents of Attacks[19]

The State of Connecticut's Department of Emergency Services and Public Protection / Division of Emergency Management and Homeland Security (CT DESPP/DEMHS) and the Connecticut Intelligence Center (CTIC) are providing this document as a guide for reporting cyber incidents within the state. A cyber incident can be reported at various stages; however, those that involve the transferring of money are time sensitive. Notifying CTIC is critical to the state's ability to combat cyber actors and understand threats. When reported, this information will be used to brief task force members, to identify and share trends, and disseminate products that can help defend against further attacks.

What to Report: To identify the cyber trends in Connecticut and across the country, CTIC requests that all cyber incidents, even unsuccessful attempts, are reported to CTIC. Helpful information includes name and contact information (phone number, email address); location of the incident (affected agency); a brief description of the incident (ransomware, spear phishing, etc.); how and when the incident was initially detected; the extent of the incident (what data was possibly affected); what response actions have already been taken; and who has been notified (local law enforcement, FBI, CTIC, etc.).

When to Report: Cyber incidents, especially those involving the transference of money, should be reported to the appropriate authorities as soon as possible. If a cyber incident is reported within 48 hours, it will greatly increase the state's ability to assist. However, agencies are encouraged to report all cyber incidents to CTIC, no matter the timing.

If the cyber incident involves the direct transference of money: It is essential for information to be submitted to the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) as soon as possible. The faster these incidents are reported to IC3, the greater probability any money that was transferred can be recovered. After incident information has been reported toIC3, contact your local Law Enforcement Agency (LEA) and CTIC. If you have any questions regarding cyber incident reporting and the communications flow, please refer to Table One on page two.

- **Internet Crime Complaint Center (IC3)** - https://www.ic3.gov/

If the cyber incident does not involve the transference of money: The affected agency should first notify their local LEA, then CTIC. This allows the local LEA to collect initial information and assign a case number, while also providing CTIC the opportunity to simultaneously share the reported

[19] https://cirma.ccm-ct.org/pdf/cyber%20security%20resources/ctcyberincidentreportingsheet_rev01062020.pdf

issue with all its partners. Municipalities, tribal nations, or private sector entities can report cyber incidents to the state at:

- **Connecticut Intelligence Center (CTIC)**
  Email: ctic.cyber@ct.gov
  Phone:(860) 706-5500
- **Cyber Crimes Investigation Unit (CCIU)**
  Email: cybercrime@ct.gov
  Phone:(860) 685-8450

To assist the State of Connecticut Intelligence Center and CIRMA, the answers to the following questions should be obtained: [20]

- Can you describe what was anomalous about the activity you observed?
- When did this start?
- Is it ongoing or has it been resolved?
- What systems are impacted by this?
- Were there any malicious files identified on the network?
- Are there any suspicious IP addresses or domains that have been identified?
- Have you identified initial access?

State of Connecticut's Cyber Disruption Response Plan (CDRP)

CTDESPP/DEMHS developed the CDRP, which describes the framework for cyber incident response coordination among state agencies, federal/local/tribal governments, and public and private sector entities: https://portal.ct.gov/-/media/DEMHS/_docs/Plans-and-Publications/EHSP0006-Cyber-Disruption-Response-Plan-2018.pdf?la=en.

This plan establishes the state's Cyber Disruption Task Force (CDTF), which is a group of subject matter experts from various disciplines involved in cyber preparedness, detection, alert, response, and recovery planning and implementation activities. Upon detection of an impending threat or significant event within the state or on the state's computer network, the CDTF may be activated to determine appropriate actions to respond to, mitigate, and investigate damages. If an event overwhelms a local community or is widespread, the State Emergency Operations Center (SEOC) may be opened to coordinate a unified response.

Taken from the CDRP, Table 1 outlines the communications flow for reporting cyber incidents, and Table 2 provides the Cyber Security Threat Matrix. Once notified, CTIC will make all appropriate notifications to its partners as outlined in Table 1 below. State agencies experiencing a significant cyber event must report it to the CT Department of Administrative Services/Bureau of Enterprise Technology (CT DAS/BEST) and to their Information Technology Unit. Entities should also contact their trusted partners as appropriate (e.g., cyber insurance providers, legal counsel, etc.).[21]

[20] Digital Dave Palmbach, Intelligence Analyst – Cyber, Conn. Intelligence Center

[21] https://cirma.ccm-ct.org/pdf/cyber%20security%20resources/ctcyberincidentreportingsheet_rev01062020.pdf

Table 1: Communications Flow for Cyber Security Threats at Levels Emergency, Severe or High (Likely to Impact Public Health, Safety or Confidence)

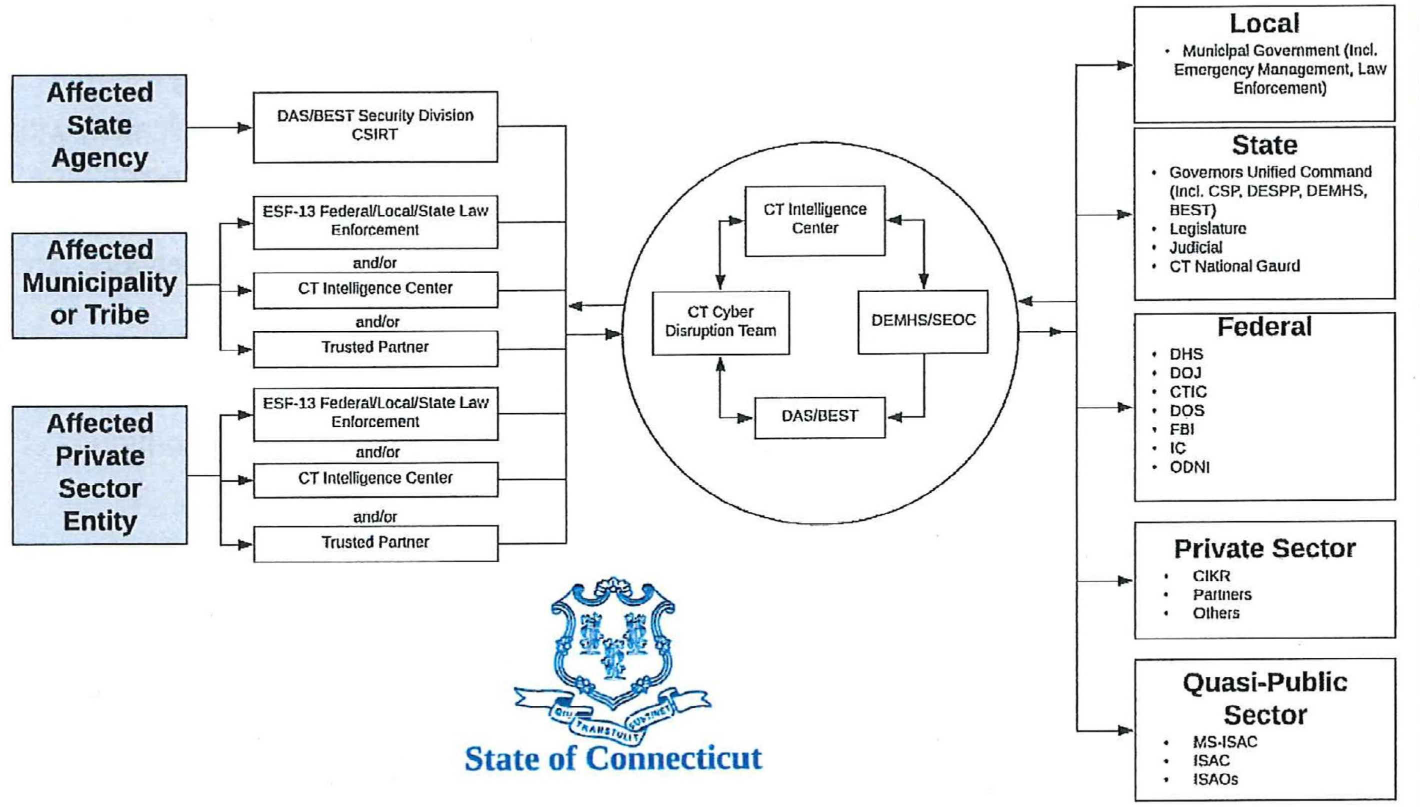
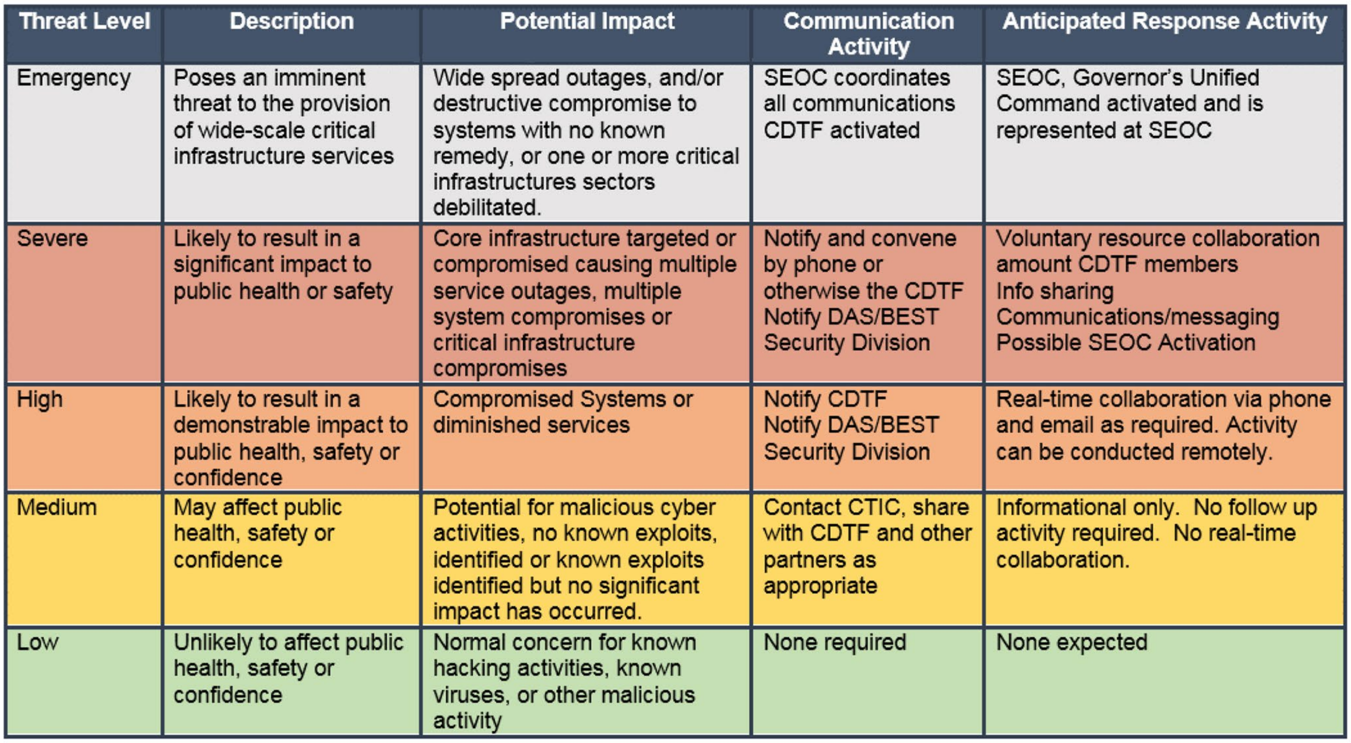


Table 2: Connecticut Cyber Security Threat Matrix.[22] The Connecticut Cyber Security Threat Matrix consists of 5 district levels, which are affected by internal and external cyber security events. The matrix provides general guidance of the communication and anticipated responses activities for each threat level.



Threat Level	Description	Potential Impact	Communication Activity	Anticipated Response Activity
Emergency	Poses an imminent threat to the provision of wide-scale critical infrastructure services	Wide spread outages, and/or destructive compromise to systems with no known remedy, or one or more critical infrastructures sectors debilitated.	SEOC coordinates all communications CDTF activated	SEOC, Governor's Unified Command activated and is represented at SEOC
Severe	Likely to result in a significant impact to public health or safety	Core infrastructure targeted or compromised causing multiple service outages, multiple system compromises or critical infrastructure compromises	Notify and convene by phone or otherwise the CDTF Notify DAS/BEST Security Division	Voluntary resource collaboration amount CDTF members Info sharing Communications/messaging Possible SEOC Activation
High	Likely to result in a demonstrable impact to public health, safety or confidence	Compromised Systems or diminished services	Notify CDTF Notify DAS/BEST Security Division	Real-time collaboration via phone and email as required. Activity can be conducted remotely.
Medium	May affect public health, safety or confidence	Potential for malicious cyber activities, no known exploits, identified or known exploits identified but no significant impact has occurred.	Contact CTIC, share with CDTF and other partners as appropriate	Informational only. No follow up activity required. No real-time collaboration.
Low	Unlikely to affect public health, safety or confidence	Normal concern for known hacking activities, known viruses, or other malicious activity	None required	None expected

[22] https://gallery.mailchimp.com/66658e65d29a7fe9d6027bdd6/files/5fb7c14a-85ec-4d58-94a0-fac73a7004af/Cyber_Quick_Reference_Charts_Jan_2019.pdf

V. The Importance of Cyber Security

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism.

Types of Municipal Threats

Ransomware[23]

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand a ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among municipalities and public-school districts, targeting and affecting their critical infrastructure. Ransomware incidents can severely impact these organizations, leaving them without the data they need to operate and deliver mission-critical services to their communities.

Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data (Cyber Extortion) if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding $1 million.

Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted municipalities and school districts. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for CIRMA members large and small.

The Cybersecurity and Infrastructure Security Agency (CISA) and the MS-ISAC have developed a set of recommended best practices designed to help manage the risk posed by ransomware and support a coordinated and efficient response to a ransomware incident. These practices are industry standards, however are guidelines that should be considered and applied to the extent possible based on the availability of organizational resources.[23]

Proper Backups – It is critical to maintain backups of data and to test your backups regularly. Having current and up-to-date backups is the most effective method for recovering from a ransomware attack without paying the ransom.

- **Consider following the 3-2-1 strategy.** As a best practice, you should have;
    - Three (3) copies of your data,

[19] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

- On two (2) additional and different platforms,
- With one (1) of those platforms being segregated from all other networks.

Create and maintain a cyber incident response plan – Being able to respond appropriately to all incidents is an important factor that can save you time and money, as well as help with the reputational risks associated with a cyber-attack. Having a strategic response plan can help you prioritize next steps during an escalating situation.

Creating a cyber incident response plan is imperative to the remediation of your incident. This predetermined plan will clearly establish the response expectations for every employee up and to the person designated to manage the incident. This allows for the response to quickly and efficiently identify and contain suspected malware, ultimately reducing the amount of time that business-critical servers are non-operational.

The plan will also need to establish a clear expectation for communications and logistics working with those third parties who can assist you in restoring your data. In addition, information about the cyber incident must be shared with executive leadership, the board of directors, your insurance company, legal departments, public relations teams, and other affected departments. For these reasons, it is important to pre-identify the necessary roles for the purpose of incident response.

Understanding what required knowledge and skillsets should be in place prior to the need for an incident response. Individuals with the required knowledge and skillsets should be available at all times to respond to an incident. A single individual may perform several roles concurrently. Members of an incident response group may or may not participate in a similarly labeled group in their day-to-day work. Specific incident response will dictate which roles are necessary and activated.[24]

- To assist Connecticut Municipalities and School Districts, the State of Connecticut has established a cyber security resource page. The below mentioned site is designed to provide resources for all levels of Connecticut users, from home computing to businesses and government organizations. These are links to recommendations and "best practices" from a variety of sources that can improve understanding of the cyber environment and how to use that environment more securely.
  - These resources can be found at: https://portal.ct.gov/connecticut-cybersecurity-resource-page

Conduct regular vulnerability scanning – This will assist in identifying and addressing vulnerabilities, especially those on internet-facing devices, to limit the attack surface.[25]

- CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: https://www.cisa.gov/cyber-resource-hub

Social engineering – Cybercriminals utilize social engineering techniques to generate detailed information to assist them with their phishing tactics in the hopes of gaining unauthorized access to the municipalities' or school districts' networks. Phishing remains the most common type of attack delivery method and infection method for malware and ransomware.

With the increased utilization of mobile devices and working from home, cybercriminals are taking the increased online activity to exploit businesses and employees. For this reason, it is ever more important to safeguard your personal and professional information and be vigilant of suspected emails and requests or calls requesting from individuals with compelling stories. Some types of requests consist of;

- Receiving a call requesting verification of personal information
- Emails or text messages written with a sense of urgency asking for your help
- Receiving notifications from organizations that you won prizes
- Internal email from staff that is asking for materials of sensitive information
- Communications with poor grammar, misspellings, etc.
- Communications with generic sender information

- Example (text message)
  Dear First name Last Name, our delivery truck was at your house a couple of hours ago: address city. You weren't at home! We still have your parcel ready for delivery! When do you want us to try again? Inform us here: link XXXXXXXXXXXXXXXXXXXXXX

- Unrecognizable email address that is not associated with the person's name
- Links that direct you to a location other than intended

Phishing

Phishing is an attempt by a cybercriminal to gain unauthorized access to the municipality and school district networks. Cybercriminals may try to entice users to access seemingly legitimate websites, click on links and other online platforms that they control. Cyber actors may also make requests for money, charitable donations, and disaster relief funds. End-users can deploy several strategies to reduce the likelihood of falling victim to cyber actors;

- Be suspicious of emails from foreign addresses or attachments
- Practice internet safety and good hygiene, visiting only familiar websites
- Doublecheck source emails
- 'When in doubt, don't click it.'

Phishing exploits can lead to:

- Disclosure of sensitive information
- Business interruptions
- Hacking, malware & unauthorized access (RDP, forward-facing servers)
- Financial fraud

CIRMA.org

Connecticut Interlocal Risk Management Agency
545 Long Wharf Drive, 8th Floor, New Haven, CT 06511

CIRMA